International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.279-288
http://dx.doi.org/10.14257/ijsia.2013.7.5.26

An Adaptive Method for Source-end Detection of Pulsing DoS Attacks

Ming Yu

School of Information and Communication Engineering, Dalian University of Technology, Dalian, China
yu_ming1111@dlut.edu.cn

Abstract

The intermittent attacking behavior of pulsing denial of service (PDoS) attacks poses a real challenge to the existing DoS detection methods. In this paper, an adaptive method is presented to meet this challenge. Three features distinguish this method from others. (i) No assumption is made on the distribution of the traffic samples. (ii) Automatic adjustment of the detection threshold according to the traffic conditions. (iii) Timely detection of the end of a PDoS attack. Simulation results validate the efficacy of the proposed method in source-end detection of PDoS attacks. They show (i) the minimum malicious traffic that can be detected by the proposed method is about 20% of the background traffic, under the requirements for detection delays of the start and the end of a PDoS attack are within 3 observation periods; (ii) the proposed method is more sensitive to pulsing SYN flooding traffic than it is to pulsing UDP flooding traffic.

Keywords: *Pulsing denial of service, adaptive detection, anomaly detection, network security*

1. Introduction

At SIGCOMM 2003, Kuzmanovic and Knightly proposed a new generation of DoS attacks, which could decrease the throughput of normal TCP traffic by periodically sending high-volume traffic in a short period. They named it "shrew attack" [1]. By further and deep study on shrew attacks, X.Luo *et al.*, proposed a generic definition of PDoS (Pulsing Denial of Service) [2]. That is, a DoS attack can be called a PDoS attack only if its attack traffic is sent in an intermittent way. By this definition, a shrew attack is considered as a kind of PDoS attacks. Different from traditional DoS attacks, PDoS traffic is sent periodically and lasts for a short time within each attacking period. Therefore, it is more difficult to detect PDoS attacks.

According to the different deployment locations, an autonomous DoS defense systems can be classified into source-end defense, victim-end defense and intermediate-network defense [3]. Among them, source-end refers to those networks that unwittingly host attacking machines; victim-end refers to the target network or the network that hosts the target machines; intermediate-network means the infrastructure between the attacking machines and the target. In recent years, source-end defense against DoS attacks has been a hotspot in network security. Several methods have been proposed for anomaly detection of the source-end traffic. Among them, the one used in the D-WARD system [4, 5] is widely accepted. It adopts a set of legitimate traffic models to identify legitimate traffic and detect or constrain malicious traffic. Unfortunately, these models need to be updated periodically and therefore cannot adapt to the frequent changes in network traffic. This paper expatiates on our latest

Manuscript received ; revised ; accepted .

ISSN: 1738-9976 IJSIA

study on source-end defense against PDoS attacks.

Symmetry is an obvious phenomenon in two-way communications that follow a request/response paradigm, such as HTTP traffic, DNS traffic, NTP traffic and some types of ICMP traffic. In these communications, one party sends a request to its peer party, and waits for a reply before sending any more packets. For such communications, it is anomalous to observe an aggressive sending rate coupled with a low response rate. Usually, such an anomalous event may indicate that some local hosts are involved in an attack. A source-end defense system may be deployed to detect those anomalies that disrupt the symmetry in these two-way communications [6, 7], but it is now challenged by the subtlety and complexity of the PDoS traffic, and the bottleneck is how to select thresholds to adapt to the variability of traffic samples.

In this paper, a nonparametric adaptive method is presented to meet this challenge. Three distinct features make this method different from others in detection of DoS traffic. (i) No assumption is made on the distribution of the traffic samples. (ii) Automatic adjustment of the detection threshold according to the traffic conditions. (iii) Timely detection of the end of an anomalous event. Rest of this paper is organized as follows. Section 2 gives a brief overview of related works on PDoS detection methods. Section 3 presents the design of an adaptive method for source-end detection of PDoS attacks. Section 4 presents the simulation results on five real traffic traces. Section 5 concludes this paper.

2. Related Works

In a few papers [8-11], several methods are proposed for anomaly detection when distributions of the traffic samples involve unknown parameters. Although these methods are successful in some conditions, two shortcomings of them are exposed when used in anomaly detection of network traffic. The first one is all the methods are designed with fixed configurations, which can not adapt to the frequent changes of network traffic. The second one is they all require a parametric model for the observations so that corresponding probability distribution functions can be applied to the design and analysis of these methods; in practice, however, it is usually very difficult to have a prior knowledge about the distribution of network traffic. Therefore, it is of crucial importance to design an “intelligent” detection method which can automatically adjust its parameters to achieve the best performance possible and work without a prior knowledge about the distribution of the observations, that is, it is nonparametric.

Luo and Chang proposed a two-stage detection system to detect PDoS attacks on the receiver side [2]. Their method is based on the presence of two types of traffic anomalies induced by PDoS attacks: periodic fluctuations in the inbound TCP data traffic and a decline in the trend of the outbound TCP acknowledgement (ACK) traffic. In the first stage, the detection system monitors the inbound data and outbound ACK traffic using discrete wavelet transform. In the second stage, a nonparametric CUSUM algorithm is employed to detect the anomalies. Experiment results show the system is effective in detecting PDoS attacks with constant attack periods. However, it is ineffective in detecting flooding-based DoS attacks because such attacks will not cause periodic fluctuations in TCP traffic.

Hussain *et al.*, proposed to differentiate between single-source and multi-source DoS attacks [12] by analyzing spectrum of the network traffic. Chen *et al.*, found the power spectrum density of a traffic stream containing shrew attacks has much higher energy in low-frequency band as compared with legitimate traffic. Based on this observation, they proposed a spectral template matching method to detect shrew attacks [13, 14]. However, all these spectrum-based methods are ineffective in detecting PDoS attacks with different attacking frequencies and intervals.

Sun *et al.*, proposed to detect shrew attacks using a dynamic time warping method which is divided into two stages [15]. In the first stage, autocorrelation is used to extract the periodic patterns in the inbound network traffic and eliminate the problem of time shifting. In the second stage, a slightly modified dynamic time warping algorithm is used to detect the signature of a shrew attack based on its autocorrelation coefficient. However, performance of this method is unsatisfactory when used in detecting PDoS attacks which are not separated by a constant interval. Moreover, such methods are ineffective in detecting flooding-based DoS attacks because the assumed square-wave patterns in such methods do not exhibit in the traffic under attack.

The D-WARD system is designed and implemented for source-end defense of DoS attacks. It adopts a useful metric that computes ratio of the inbound TCP traffic to the outbound TCP ACK traffic in detecting DDoS attacks [4]. Such a metric is also adopted in the Vanguard DoS detection system [16, 17]. In both systems, however, a fixed ratio of the inbound TCP traffic to the outbound TCP ACK traffic is used to distinguish an attack flow from legitimate ones, which cannot adapt to the frequent changes in network traffic. Therefore, it is of crucial importance to design an "intelligent" detection method which can automatically adjust its detection parameters to adapt to the changing network conditions.

In [7], I have proposed a nonparametric adaptive CUSUM method for network anomaly detection. This paper expatiates on my latest study of source-end defense against PDoS attacks. Its main contribution is to propose an adaptive detection method for source-end detection of PDoS attacks.

3. Design of an Adaptive Method for Source-end Detection of PDoS Attacks

3.1. Problem Formulation

Let us begin by giving the problem formulation of PDoS detection before we go deep into the design of the proposed adaptive detection method. Suppose $X=\{x_n, n=1,2,\cdots\}$ is a sequence of independent random variables observed sequentially, and $x_n=[(O_n-I_n)/O_n]^+$. Respectively, O_n and I_n denote the number of outgoing requests and incoming replies collected within the n^{th} observation period which is represented by the symbol T. x^+ is equal to x if $x>0$ and 0 otherwise.

For legitimate traffic, O_n is approximately equal to I_n, thus we have $x_n\approx 1$. Normally, the mean of X (denoted by μ_X) is stable and close to 1. This conclusion has been referred by Mirkovic [4]. It is also supported by our analysis on some real traffic datasets collected at Dalian University of Technology. Figure 1 gives the result of our analysis on one of those datasets. As we can see, an anomalous event occurs and μ_X is increased at a certain moment (random and unknown). When the anomaly ends, the mean of X is decreased to normal. Figure 2 illustrates this process. However, no prior knowledge is known about the probability distribution function of X. The aim of a PDoS detection method is to accurately detect the start and the end of the PDoS attack as soon as possible.

3.2. Design of the Method

Firstly, the sliding window mechanism is adopted to alleviate the non-stationary influence of X on the method. Size of the window is denoted by N, and elements in the window are denoted by w_n^j, where $0\le j\le N-1$ and $n=0, 1, 2, \ldots$. Usually, w_0^j is initialized by $w_0^j = a$, where

$0 \le a \le 1$. In practice, a can be empirically set and it does not have much influence on the performance of the method.

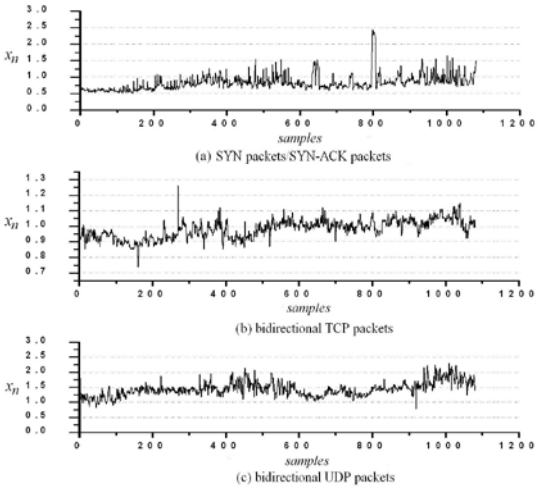

Figure 1. Analysis of x_n based on One of the Real Traffic Dataset

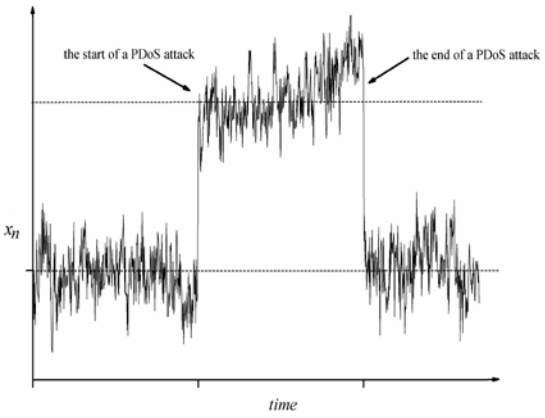

Figure 2. Illustration of PDoS Detection

Secondly, the test statistic t_n is constructed as

$$t_n = \sum_{j=0}^{N-1} (x_n - w_{n-1}^j)^2, n = 1,2,\cdots \quad (1)$$

Thirdly, the detection threshold for raising an alarm on the start of a PDoS attack is set as

$$G_n^{\text{start}} = N \times ((1 - \overline{w}_{n-1}) \times \delta)^2 \quad (2)$$

where $\overline{w}_{n-1} = (\sum_{j=0}^{N-1} w_{n-1}^j)/N$ and δ is the normalized intensity of the aggressive sending rate. δ is defined as $\delta = O_A/(O_A + \overline{O}_{n-1})$, where O_A denotes the number of aggressive outgoing requests in an observation period and $\overline{O}_{n-1}$ denotes the averaged number of normal outgoing requests in the $n-1^{\text{th}}$ observation period. To reduce false alarms, threshold violations are counted. If the counter (denoted by Num) reaches a specified number τ_s, an alarm is raised and the counter is reset to zero. Detection results are denoted by d_n, by which d_n=1 is for raising alarms and d_n=0 for no alarms. Update of elements in the sliding window depends on the detection results, as can be seen from the codes in Table 1, which gives the key codes for judging the start of a PDoS attack.

Lastly, another two thresholds, G_n^{end} and *G_saved*, are used in canceling an alarm. *G_saved* is set when an alarm is raised, as can be seen in Table 1. G_n^{end} is set as $G_n^{\text{end}} = 0.5 \times N \times ((1 - \overline{w}_{n-1}) \times \delta)^2$. The same counter used for reducing false alarms is also used here to avoid missing alarms. An alarm cannot be canceled until the counter reaches another specified number τ_e. In this proposed method, τ_s and τ_e are respectively considered as the requirements for detection delays of the start and the end of a PDoS attack. Codes for judging the end of an anomalous event are given in Table 2.

4. Simulations and Analysis

Five real traffic traces are used to validate the proposed method. Three of them were collected by a Endace® DAG card at Dalian university of technology (DLUT) with an OC-48c PoS link connected to CERNET. The other two were collected by the NLANR group at the University of Auckland (Auck) with an OC3 Internet access link. A summary of these traces is given in Table 3.

Table 1. Key Codes for Judging the Start of a PDoS Attack

```
IF ( t_n ≥ G_n^start and x_n ≥ w̄_{n-1} )
{ Num++;
  IF ( Num == τ_s )
  { d_n=1; Num=0;
# save the current threshold.
    G_saved = G_n^start ;
    FOR (j=0; j<N; j++)
      {
# save elements in the current window.
        r[j] = w_{n-1}^j ;
# reset elements in the sliding window.
      w_n^j = x_n ;
      }
  }
}
ELSE
{ Num-- IF(Num>0);
  FOR(j=0; j<N−1; j++)
  { w_n^j = w_{n-1}^{j+1} ; }
  w_n^{N-1} = x_n ;
}
```

Table 2. Key Codes for Judging the End of a PDoS Attack

```
tmp=0;
IF ( t_n ≥ G_n^end and x_n < w̄_{n-1} )
{ FOR(j=0; j<N; j++)
    tmp = tmp + (x_n − r[j])^2 ;
  IF( tmp ≤ G_saved )
  { Num++;
    IF ( Num == τ_e )
    { d_n=1; Num=0;
      FOR(j=0; j<N; j++)
      { w_n^j = x_n ; }
    }
  }
}
ELSE
{ Num-- IF(Num>0);
  FOR(j=0; j<N−1; j++)
  { w_n^j = w_{n-1}^{j+1} ; }
  w_n^{N-1} = x_n ;
}
```

Table 3. Summary of the Real Traffic Traces used in the Experiments

Trace	Start time	Run length	IP headers
DLUT-1	09:10:01,Aug 11, 2012	02:46:01	115 million
DLUT-2	09:10:02, Sep 12, 2012	01:30:05	176 million
DLUT-3	14:18:59, Oct 21, 2012	02:00:00	130 million
Auck-1	18:59:16, Jun 8, 2001	05:00:43	14 million
Auck-2	12:00:00, Jun 9, 2001	06:00:00	22 million

Firstly, simulations on source-end detection of SYN flooding attacks were carried out to illustrate the efficacy of the proposed method. In these simulations, the aggressive flooding rates were assumed constant after the attacks were launched. During an attack, the pulsing attack traffic lasted 10 minutes, and then it stopped for 5 minutes. Some results of the simulations on the trace of DLUT-1, Auck-1 and Auck-2 are presented in Figure 3-Figure 5. For the DLUT-1 trace, four pulsing attacks were launched respectively at the 105th, 210th, 315th and 420th observation periods, and each attack persisted for 30 minutes. For the Auck-1 trace, five pulsing attacks were launched respectively at the 75th, 255th, 435th, 615th and 795th observation periods, and each attack persisted for 45 minutes. For the Auck-2 trace, six pulsing attacks were launched respectively at the 75th, 255th, 435th, 615th, 795th and 975th

observation periods, and each attack persisted for 45 minutes. The observation period T was set to 20 seconds. Other parameters involved in the proposed method were set as follows: N=4, α=0.1, δ=0.2 and τ_s=τ_e=3.

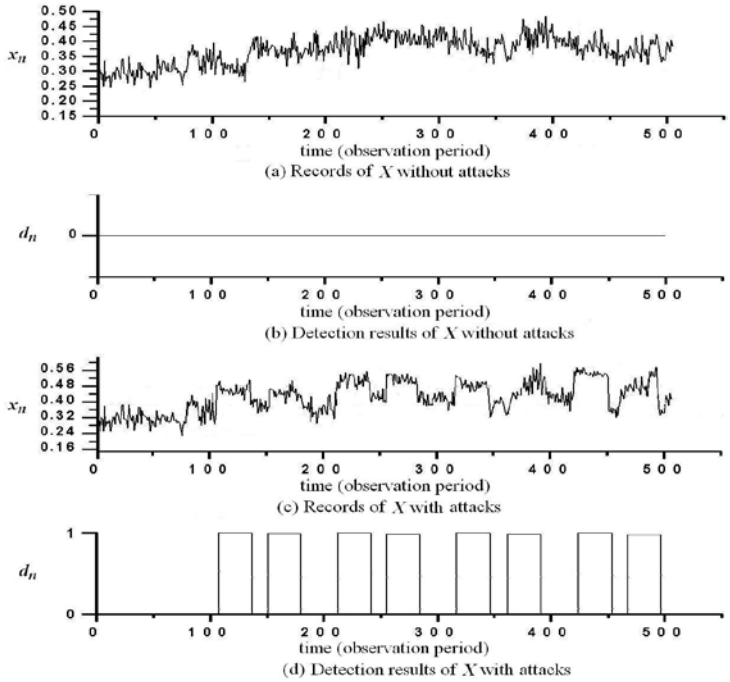

Figure 3. Simulation Results on DLUT-1 Trace

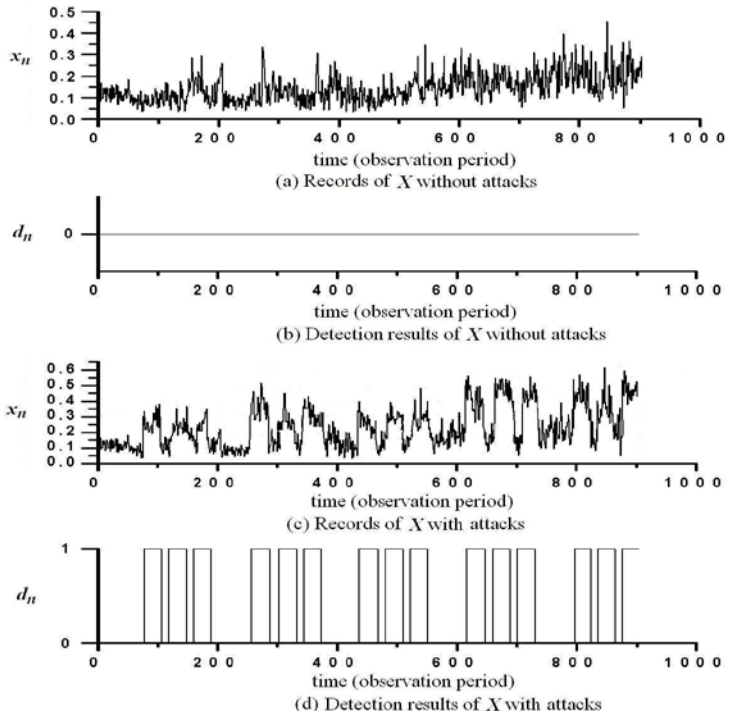

Figure 4. Simulation Results on Auck-1 Trace

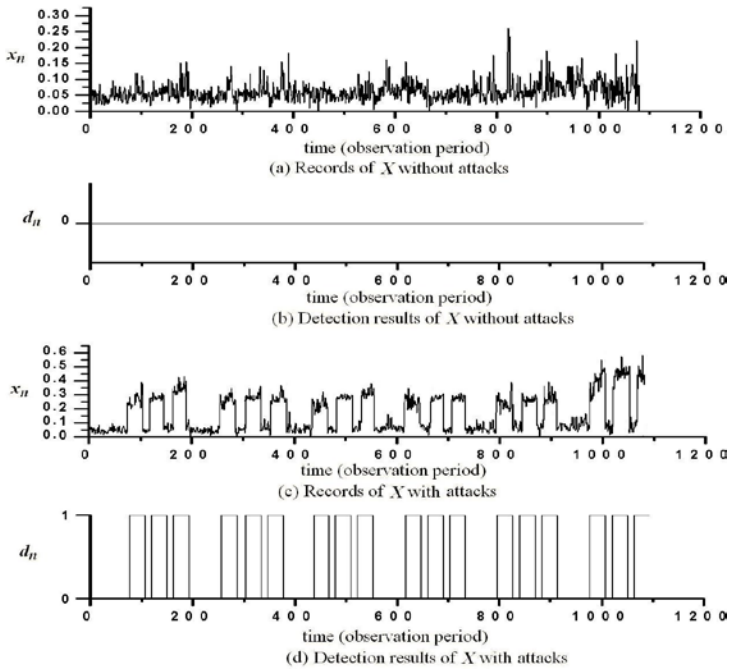

Figure 5. Simulation Results on Auck-2 Trace

Secondly, detailed information about the simulations is presented to show the efficiency of the proposed method. For each trace, two types of PDoS traffic were included. Respectively, they are SYN flooding traffic and UDP flooding traffic. All the attacks are launched every 15 minutes, and the bursting time of each attacking machines is 10 minutes. Other parameters involved in the proposed method were set as follows: N=4, α=0.1, δ=0.2, and τ_s=τ_e=3. In this paper, we emphasize on studying the detection of low intensity attacks with the detection delays kept as short as possible. Table 4 and Table 5 give the averaged detection results on pulsing SYN flooding traffic and pulsing UDP flooding traffic by the proposed method after 30 experiments on each trace.

Table 4. Averaged Detection Results on Pulsing SYN Flooding Traffic

	DLUT-1	DLUT-2	DLUT-3	Auck-1	Auck-2
$\overline{\delta}$	0.217	0.199	0.190	0.191	0.209
$\overline{\tau}_s(T)$	3.1	3	3.1	3.1	3.2
$\overline{\tau}_e(T)$	3.1	3	3.1	3.1	3.2

Table 5. Averaged Detection Results on Pulsing UDP Flooding Traffic

	DLUT-1	DLUT-2	DLUT-3	Auck-1	Auck-2
$\overline{\delta}$	0.223	0.215	0.23	0.216	0.207
$\overline{\tau}_s(T)$	3.3	3..2	3	3.2	3.1
$\overline{\tau}_e(T)$	3.3	3.1	3	3.1	3.1

Two conclusions can be drawn from both tables.

(1) Under the requirement that the detection delays be within one minute, the lowest

intensity of the attacks that can be detected by the proposed method is 0.199. This result excels those obtained in [18, 19] where the lowest intensity of the attacks that can be detected by the nonparametric CUSUM method is 0.25.

(2) The proposed method is more sensitive to the pulsing SYN flooding traffic than the pulsing UDP flooding traffic. This is because the proportion between outgoing SYN packets and incoming ACK packets is more regular and closer to 1.

In fact, the low intensity of the PDoS attacks that can be detected by the proposed method depends on the users' requirements on δ, which reflects the anomalies of the PDoS attacks. As an example, Table 6 gives another group of the detection results on pulsing SYN flooding traffic when δ=0.15 and other parameters were kept unchanged. As we can see, the lowest intensity of the attacks that can be detected is further decreased. However, we think δ=0.15 is insufficient to discriminate between the attacks and the normal fluctuation of legitimate traffic so far as SYN flooding attacks are concerned. The experimental results show the choice of δ completely depends on the related applications and it rests with the users.

Table 6. Averaged Detection Results on Pulsing SYN Flooding Traffic when δ=0.15

	DLUT-1	DLUT-2	DLUT-3	Auck-1	Auck-2
$\overline{\delta}$	0.154	0.164	0.133	0.138	0.145
$\overline{\tau}_s(T)$	3.5	3.2	3.6	3.8	3.2
$\overline{\tau}_e(T)$	3.2	3.1	3.1	3.1	3.5

5. Conclusion

In this paper, an adaptive method is presented for source-end detection of PDoS attacks. This method requires little knowledge of the network traffic except a loose symmetry between the outgoing packets and the incoming packets. Three distinct features of this method are emphasized. Firstly, no assumption is made on the distribution of the traffic samples. Secondly, it succeeds in implementing a self-adjusting detection threshold, which makes it adapt to various traffic conditions. Thirdly, it reacts quickly to the end of the PDoS attacks. Experiments on real traffic traces show the efficacy of this method in detecting low intensity PDoS attacks. In the future, we plan to employ this method in detecting other DDoS attacks such as DRDoS, SYN/ACK attacks and RESET attacks.

Acknowledgements

This work was supported by (1) National Natural Science Foundation of China (Grant No.61172059); (2) the Scientific Research Foundation for Ph.Ds of Liaoning Province, China (Grant No.20111022).

References

[1] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted Denial of Service Attacks: the Shrew vs. the Mice and Elephants", Proceedings of ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Karlsruhe, Germany, **(2003)** August 25-29.

[2] X. Luo, and R. Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense", Proceedings of Network and Distributed System Security Symposium, San Diego, USA, **(2005)** February 3-4.

[3] Y. Ming, "A Nonparametric Adaptive CUSUM Method and Its Application in Source-End Defense against SYN Flooding Attacks", WuHan University Journal of Natural Science, vol. 16, no. 5, **(2011)**, pp. 414-418.

[4] J. Mirkovic and P. Reiher, "D-WARD: A Source-End Defense Against Flooding Denial-of-Service Attacks", IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 3, **(2005)**, pp. 216-232.
[5] O. Pal, P. Jain, S. Goyal, Zia Saquib and B. L. Menezes, "Intrusion Detection Using Graph Support: A Hybrid Approach of Supervised and Unsupervised Techniques", International Journal of Advancements in Computing Technology, vol. 2, no. 3, **(2010)**, pp. 114-118.
[6] X. Liu, X. Yang and Y. Xia, "NetFence: preventing internet denial of service from inside out", SIGCOMM Computer Communication Review, vol. 40, no. 4, **(2010)**, pp. 255-266.
[7] M. Yu, "A nonparametric adaptive CUSUM method and its application in network anomaly detection", International Journal of Advancements in Computing Technology, vol. 4, no. 1, **(2012)**, pp. 280-288.
[8] S. Ehlerta, D. Geneiatakisb and T. Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks", Computers & Security, vol. 29, no. 2, **(2010)**, pp. 225-243.
[9] H. K. Yi, P. K. Park, S. Min and J. C. Ryou, "DDoS Detection Algorithm Using the Bidirectional Session", Communications in Computer and Information Science: Computer Networks, vol. 160, **(2010)**, pp. 191-203.
[10] Z. Li, Y. Gao and Y. Chen, "HiFIND: A high-speed flow-level intrusion detection approach with DoS resiliency", Computer Networks, vol. 54, no. 8, **(2010)**, pp. 1282-1299.
[11] O. I. Sheluhin, A. A. Atayero and A. B. Garmashev, "Detection of Teletraffic Anomalies Using Multifractal Analysis", International Journal of Advancements in Computing Technology, vol. 3, no. 4, **(2011)**, pp. 174-182.
[12] A. Hussain, J. Heidemann and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks", Proceedings of ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Karlsruhe, Germany, **(2003)**August 25-29.
[13] Y. Chen and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks Using Spectral Analysis", Journal of Parallel and Distributed Computing, vol. 66, no. 9, **(2006)**, pp. 1137-1151.
[14] Y. Chen and K. Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks", Proceedings of IEEE International Conference on Communications, Glasgow, Scotland, **(2007)** June 24-28.
[15] H. Sun, J. C. S. Lu and D. K. Y. Yau, "Defending against Low-rate TCP Attacks: Dynamic Detection and Protection", Proceedings of the 12th IEEE International Conference on Network Protocols, Berlin, Germany, **(2004)** October 5-8.
[16] X. Luo, E. W. W. Chan and R. K. C. Chang, "Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals", EURASIP Journal on Advances in Signal Processing, vol. 2009, **(2009)**, pp. 1-13.
[17] C. W. Zhang, Z. P. Cai, W. F. Chen, X. Luo and J. Yin, "Flow Level Detection and Filtering of Low-rate DDoS", Computer Networks, vol. 56, no. 15, **(2012)**, pp. 3417-3431.
[18] V. A. Siris and F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks", Proceedings of GLOBECOM, Dallas, USA, **(2004)** November 29-December 3.
[19] P. Tao, C. Leckie and K. Ramamohanarao, "Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring", Proceedings of NETWORKING, Athens, Greece, **(2004)** May 9-14.

Authors

Ming Yu received the BS degree in electronics engineering in 1998 from Shandong University, China. He received the MS degree and Ph.D degree in information and telecommunication system in 2004 and 2008 from Xidian University, China. He is currently an associate professor in Dalian University of Technology, China. He is also a member of IEEE Computer Society. So far, he has 15 papers published in international journals. His research interests include network security, cloud computing and DoS defense.